

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CONVERGEN ENERGY LLC, L'ANSE WARDEN
ELECTRIC COMPANY, LLC, EUROENERGY
BIOGAS LATVIA LIMITED, and LIBRA CAPITAL
US, INC.

Plaintiffs,

-against-

STEVEN J. BROOKS, NIAN TICVISTA ENERGY
LLC, GREGORY MERLE, RIVERVIEW ENERGY
CORPORATION, DANIEL ESCANDON GARCIA,
RAMON URIARTE INCHAUSTI, CHIPPER
INVESTMENT SCR, SA, URINCHA SL, THEODORE
JOHN HANSEN, BRIAN R. MIKKELSON, and
CONVERGEN ENERGY WI, LLC,

Defendants.

Civil Action No. 1:20-cv-03746 (LJL)

**EMERGENCY DECLARATION
OF PHAEDRA S. CHROUSOS
IN SUPPORT OF
PLAINTIFFS' APPLICATION**

I, Phaedra S. Chrousos, declare:

1. I am the Chief Strategy Officer at Plaintiff Libra Capital US, Inc. (the "**Company**") and have been personally involved in the facts herein. I submit this affidavit in support of the motion for a temporary restraining order ("**TRO**") and preliminary injunction of Plaintiffs EuroEnergy Biogas Latvia Limited ("**Convergen Latvia**"), Convergen Energy, LLC ("**Convergen**"), L'anse Warden Electric Company, LLC (the "**Power Plant**") and the Company.

2. Plaintiffs seek emergency relief to: (i) cut off Defendants' unlawful and unauthorized access to Plaintiffs' emails and other electronic stored files; (ii) ward off a cyberattack by unknown hackers; (iii) obtain administrator access to Plaintiffs' own files, which currently Defendants unlawfully control; and (iv) recover computers and cellphones in the possession of certain defendants that contain Plaintiffs' trade secrets and other proprietary information. Among the email and data files to which Defendant have access and are at risk of

further cyberattack are Plaintiffs' trade secrets and confidential and proprietary information.

3. Defendants' unlawful access is the byproduct of their fraudulent scheme to purchase from Convergen (through undisclosed double-dealing) a renewable pellet manufacturing plant in Green Bay, Wisconsin ("**Pellet Plant**") for at least ten million dollars less than its fair market value. Three of the defendants were corporate insiders (senior executives of Plaintiffs) who orchestrated the January 2020 sale. Those double-dealing executives oversaw, managed and, ultimately, sold the Pellet Plant on behalf of Convergen to themselves (covertly) and, as part of their job responsibilities, also administered the email accounts for all Convergen affiliates prior to the sale. As part of the self-dealing transaction, the defendant insiders failed to segregate and take with them the email accounts of just the pellet plant; thus, post-sale Defendants have maintained access to not only the Pellet Plant emails but also to other Convergen entity emails and electronic files. The theft was only discovered after the email of a senior employee of Convergen Latvia was hacked. Defendants refused to provide Plaintiffs with administrator access to ward off the cyberattack despite repeated requests, eliminating any doubt about Defendants' mal intent. This motion seeks to put an end to the unlawful access and to provide Plaintiffs with much needed administrator access to their own emails and files.

A. Background

4. Plaintiffs are part of an international conglomerate headquartered in New York known as the Libra Group (the "**Group**"). The Group is a privately owned international business group that is active in 35 countries and focused primarily on energy, hospitality, real estate, shipping and aviation that traces its origin to a shipping company established in 1976.

5. The Company, a member of the Group, is a 15-year-old in-house asset management and professional service company that supports other companies that are part of the

Group, including Convergen. Convergen owns and operates a portfolio of alternative energy assets, including two cogeneration or combined heat and power (CHP) facilities in Manhattan, several biogas facilities in Latvia (Northern Europe) through Convergen Latvia, a 20 megawatt electric power plant in Michigan (the Power Plant) and formerly the Pellet Plant.

6. Prior to the sale of the Pellet Plant in January 2020, Convergen personnel based in Wisconsin at the Pellet Plant, specifically defendants Theodore John Hansen (“**Hansen**”) and Brian R. Mikkelsen (“**Mikkelsen**”), managed the email accounts for all of the Convergen entities, including all emails using the domain convergenenergy.com, lansewarden.com (for the Power Plant) and euroenergybiogas.com (for Convergen Latvia). Hansen and Mikkelsen worked directly for Steven J. Brooks (“**Brooks**”), the senior executive of the Group tasked with overseeing Convergen assets.

7. Brooks spearheaded the sale of the Pellet Plant to defendant Nianticvista Energy LLC (“**Niantic**”). The complaint sets forth the details of the fraudulent scheme. In short, unbeknownst to Plaintiffs, Brooks has a financial interest in Niantic. His underlings Hansen and Mikkelsen helped Brooks arrange for the double-dealing (and commercially unreasonable) sale of the Pellet Plant to Brooks and the other defendants (believed to be stakeholders in Niantic).

8. After the sale of the Pellet Plant, Hansen and Mikkelsen remained in Wisconsin working with the new ownership and ceased working for Convergen. As part of the Pellet Plant transaction, Brooks, Hansen and Mikkelsen (collectively, the “**Defendant Insiders**”) should have segregated and relinquished control of the email accounts of the Convergen entities, and should have maintained access to only a limited number of the Pellet Plant’s emails necessary for operations. Plaintiffs recently learned that this did not happen.

B. A Cyberattack Uncovered Defendants' Unlawful Access

9. On April 14, 2020, Alexander Strelkov (“**Strelkov**”), a senior executive at Convergen Latvia alerted the Group’s Chief Accountant, Neil Mortimer, that he just learned his email account was hacked on April 10, 2020. Strelkov explained that the hackers had obtained his password, changed his email settings, and then used his account to send a fake invoice to his accounting team to pay an unknown company in the United Kingdom. Strelkov has worked for the Group for over 15 years and the amount of data stolen from his email could be highly significant and widespread across the Group

10. As per Group protocol, the cybersecurity breach was immediately reported to the Group’s Chief Information Officer, Nikolaos Baziotis (“**Nikos**”), whose responsibility it is to ensure that the highest level of cybersecurity is maintained across all of the Group’s businesses. Nikos jumped into action and notified the Group’s Executive Board of the breach and reached out to Strelkov to access Convergen’s email account so that he could: (i) understand how long the hackers had access to Convergen Latvia’s email systems; (ii) understand if the hackers had downloaded a copy of all historical mails; and (iii) apply 2-factor authentication to the account so as to prevent future hacks.

11. To do these things, Niko needed the administrator rights to a Microsoft product known as Office 365, which Convergen used for its emails and data storage. Office 365 is a cloud-based software that includes a hosted email Exchange Server and data storage. The administrator rights are the master key that provides access and control of an Office 365 account.

12. Nikos was stunned to discover that the administrator rights to Convergen Latvia’s Office 365 account were no longer located safely in the possession of the Group but were held by Mikkelson. There was no basis for Mikkelson or anyone else associated with the

Pellet Plant to have access to, let alone maintain exclusive administrator access over, the Office 365 accounts of other Convergen entities, including the Power Plant and Convergen Latvia. The transaction, while fraudulent, did *not* include the sale or access to *any* Office 365 accounts.

13. Nikos also discovered that the Defendant Insiders did not provide Convergen with access to or a copy of the Pellet Plant emails for the period preceding the sale. Corporate records are needed for compliance and tax purposes, among other reasons.

14. Nikos' discoveries in response to the cyberattack highlighted the duplicity of the Defendant Insiders. None took the ordinary steps to ensure that emails and data were appropriately segregated between the seller (Convergen) and the buyer (Niantic). This is particularly egregious in light of the fact that after the sale, the Power Plant and Pellet Plant were parties to a long-term supply agreement (also part of the fraudulent scheme), one as the buyer and the other as the seller (*i.e.*, at arms' length). It is incongruous for one party to a contract to have access to the emails and data of the other party.

C. Defendants Deny Plaintiffs Access

15. On April 14, 2020 Nikos and Strelkov emailed Mikkelson to transfer the administrator rights to the Office 365 accounts. The next day Strelkov copied Mikkelson on an email to Nikos, advising him that a second employee at Convergen Latvia was the victim of an email hack at convergenenergy.com. Nikos advised Strelkov and his team to change their passwords and asked Mikkelson again for administrator access to log in, assess the extent of the damage caused by the hackers and apply 2-factor authentication to better secure the system.

16. For the next week, Nikos continued to email Mikkelson and reiterate the urgent request to transfer administrator access of the Office 365 accounts. Mikkelson never granted the request with respect to the Convergen and Convergen Latvia accounts. Perhaps

recognizing how inappropriate it was to have access to the Power Plant emails (an entity on the other side of contract), Mikkelson granted Nikos access to the Power Plant Office 365 account on April 22, 2020.

17. On April 20, 2020, Camilo Patrignani (“**Patrignani**”), Senior Advisor at the Company, contacted Hansen to press for the requested access. Hansen explained that “[Mikkelson] is our guru and manages all of this]” and that authorization would be needed from defendant Greg Merle (“**Merle**”), the CEO of Niantic. Patrignani then emailed Merle to ask for administrator access to the Office 365 accounts. On April 23, 2020, Merle responded that he would revert after looking into the issue.

18. The next day, when Nikos followed up with Mikkelson, Mikkelson again refused to provide administrator access and only offered to migrate the emails to a separate domain. This “solution” would allow Defendants to unlawfully maintain control over Convergen’s Office 365 account and would have deprived Convergen of: (i) the ability to investigate the cyberattack (source and damage); (ii) its rightful historical records; (iii) records and audit logs of any unlawful access post-sale; and (iv) the assurance that emails to the old domain would route to a new domain. Plaintiffs would remain at the mercy of Mikkelson. It was a meaningless offer.

19. On April 27, 2020, Patrignani followed up with Merle because he had not yet responded. On April 30, 2020, Merle finally responded to Patrignani, referring to the nonsensical domain transfer floated by Mikkelson on April 24. Camilo responded the same morning to explain, again, why administrator access was needed and why a domain transfer was separate and apart from what was urgently needed. Merle ignored this request until May 6, 2020 when he merely repeated the same domain transfer nonsense from before. Patrignani responded

immediately, explaining yet again why what Merle was saying made no sense and was woefully inadequate. Merle did not respond.

20. In a last-ditch effort, on May 11, 2020 Plaintiffs' counsel sent via email a draft complaint to Defendants: "Absent resolution of the issues raised in the attached complaint ... we will be seeking relief in a New York court, as time is of the essence due to the ongoing irreparable harm at issue." The Defendants did not respond. Plaintiffs had no choice but to file this lawsuit and motion for emergency relief. It has been more than a month since the Group learned of the cyberattack and contacted the Defendant Insiders for the needed access. Plaintiffs have been deprived of the ability to ward off more cyberattacks (*e.g.*, adding a two-factor authentication system) and assess the extent of the existing hacks.

21. Defendant Merle and the other Defendant Insiders made it blatantly obvious that they were obfuscating, obviously trying to cover up their own tracks. There is absolutely no reason for these fraudsters in Wisconsin to have access to Plaintiffs' emails – emails of the Latvia business – unless providing such access will uncover more incriminating evidence of the fraud and Defendants' unlawful access to Plaintiffs' trade secrets.

D. Irreparable Harm

22. The Office 365 accounts contain trade secrets of Plaintiffs that include but are not limited to historical and current confidential communications regarding financials, client contracts, market analysis, potential transactions, strategic discussions, and the day-to-day operations. More specifically, the Office 365 accounts detail: (i) a unique fuel mix developed over years by the Power Plant that optimizes thermal power plants; (ii) asset management protocols of distribution for a network of combined heat/power and biogas plants; (iii) unique energy contracts and documentation that Plaintiffs invested significant funds to create and reflect

years of Plaintiffs' experience. Further, Convergen must retain a copy of all historical emails for up to ten years for compliance and audit purposes under applicable United Kingdom and Latvian law.

23. Plaintiffs took several steps to protect these trade secrets. First, it required its employees to enter into confidentiality agreements limiting use of confidential information only for the purpose of performing duties as an employee. Second, the Office 365 accounts and individual email accounts are accessible only through password protected entry points. Third, the Group's Employee Handbook makes abundantly clear that employees must preserve the confidentiality of the Group's information and protect the electronic data from unauthorized access.

24. The Defendant Insiders were also required and agreed to return their company laptops and cellphones upon termination of their employment, particularly because they contained proprietary information including trade secrets. Indeed, their respective employment agreements acknowledged that each will "obtain "obtain proprietary, trade secrets and confidential information" of the Company and its affiliates that he must not disclose, and that unlawful disclosure would result in "substantial damage which will be difficult to compute" and that he "consents and agrees" the Company "shall be entitled, in addition to any other remedies it may have at law, to the remedies of injunction." None of them returned their company hardware.¹

25. I personally reminded Brooks on at least three phone calls that he must return the Group's hardware. Brooks responded that he would do so but never did even though he resides four blocks from the Group's New York office. Brooks is in possession of the

¹ The language in Hansen's employment agreement differs immaterially to Brooks' and Mikkelsen's agreements.

following devices owned by the Group, which I believe contain highly proprietary information, including investor lists, Company financials, presentations, closing documents for numerous transactions, monthly reports, accounts, spreadsheets and other confidential information and trade secrets consistent with his role as a senior investment manager for an international conglomerate:

- A. iPhone 8 - Device ID: MM6LN3NN7H2FR23UCIP9MT7L08;
- B. iPhone 11 Pro - Device ID: TG484IJEP2HVBAN405AV82M70; and
- C. Lenovo ThinkPad P50 (20EN001EUS) – 15.6” – Core i7 6820HQ Processor – 16 GB RAM – 256 GB SSD.²

26. I emailed Brooks to return the devices by February 28. Brooks did not respond, and I followed up again by email on March 3 and March 20, each time asking him to mail the devices. Finally, on March 20, Brooks responded “I unfortunately do not have access to my hardware as I am currently self-quarantining. However, as soon as I can I will bring them to the office.” In light of all of the shenanigans described above, Brooks’ response is nothing more than a stall tactic. I believe that he may be storing the devices at his alternative address at 75 Inwood Road, Darien, Connecticut.³

27. The irreparable harm to the Company is obvious. Without any basis in fact or law, the defendants are depriving Convergen of the ability to protect its own data, especially from unknown hackers. The defendants are also unlawfully granting themselves continued access to Plaintiffs’ proprietary and confidential information and trade secrets (all contained

² I believe Mikkelson and Hansen’s company laptops and cellphones contain the same type of proprietary information. We do not know the specific model numbers of their phones and laptops.

³ On May 14, 2020, an investigator called Brooks’ number to determine his location for service of the complaint. Brooks pretended to be his father in reporting that “Brooks” was not quarantining in Connecticut with his parents and no longer lived at the New York address. I know this to be a lie because, among other reasons, Brooks’ father had passed away some time ago.

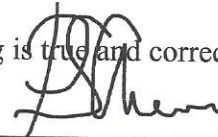
within the email files located on the Office 365 accounts). In addition to engaging in misappropriation, defendants are denying Convergen access to the email files of the Pellet Plant prior to the sale, which, as stated above, are needed for future compliance requirements. Defendants' motive for denying access is also obvious: presumably among those files are incriminating emails about defendants' fraudulent scheme.

28. In sum, Defendants have defrauded Plaintiffs, misappropriated Plaintiffs' data and are now thwarting Plaintiffs' efforts to defend itself from hackers. If Defendants are permitted to continue controlling our Office 365 accounts, our reputation, operations and confidential communications will remain in their hands while we wait for trial on this matter. Consequently, Defendants' actions are causing and, unless restrained, will continue to cause damage and immediate irreparable harm to Plaintiffs.

29. On the other hand, if Defendants are required to return the Office 365 account for Convergen Latvia and grant us administrator access to Convergen's Office 365 account so that we may securely migrate and forward our emails, data and logs, and investigate the hack, they will suffer no harm because they have no right to our data.

30. For these reasons, the facts set forth in our counsel's declaration, and the law set forth in the accompanying Memorandum of Law, it is respectfully requested that the Court grant Plaintiffs' motion for a TRO and a preliminary injunction. No prior applications for this relief have been made.

I declare under penalty of perjury that the foregoing is true and correct.



PHAEDRA S. CHROUSOS

Sworn to before me this
18th day of May, 2018